Good example of "a model-driven approach to privacy leakage identification and an...

Law, Security

Business Plan

Analyzing Baseline Privacy Requirements

This research aims to determine privacy requirements in technological environments, the way privacy by design principles help design privacy aware systems and proposes enhanced privacy framework, using a model driven solution based on Tropos methodology, and language specification for preventing privacy leakage.

The first two phases of the framework design analyze privacy guidelines and privacy requirements in existing frameworks.

For the sake of simplicity, the proposed framework concentrates only on a subset of all privacy requirements to ensure that requirements could be modeled within the given time and by using the resources, as follows,

Note: Not all privacy requirements apply to ‘ all modules’ within the system under design. Only a few apply to each module. This reduces implementation complexity.

Defining Stakeholders (Actor Model)

For a secure Tropos privacy framework implementation, all the stakeholders (entities with their interests within target system) must be identified. Few Stakeholders in any software system are, as follows,

An authentication sub-system goal is to authorize access. Here, the capabilities vary, for example, an authentication sub-system can reject data access for some users, or abstract code modules.

Determining Privacy Requirements (The Meta-Model Approach)

The Secure Tropos starts off modeling the framework using meta-model. As discussed in proposal, meta-model allows aligning the safe Tropos to the ‘ privacy framework’, which further could readily be applied to any system in design with intended privacy goals. The meta-model integrates and formalizes the relationship between the threats, users, actors, stakeholders, and other entities in the system, as determined by the actor-model in the prior phase. Meta-model makes note of the relationship between entities and actors (as well as, which of the above security requirement apply to which component).

Meta-model also defines the ‘ privileges' various users (stakeholders) posses over the other sub-systems and the actions they can perform, and that how various sub-systems acknowledge responses to the request for ‘ data access' and ‘ actions' to be performed.

For research, a full meta-model must be defined for a complete description of entities, actors and relationships, and the effectiveness of the established framework, in preventing the privacy. Each of the privacy requirements in proposed framework defines its set of actors, entities, capabilities, relationships, and actions.

Secure Tropos Implementation (using SI* Language, Capability Diagram and Rules)

Here, the capability ID corresponds to another table (being the primary key for that table), which defines the ability itself.

For visualization of the privacy requirements and privacy plan, the capability diagrams are used. Those diagrams visualize the various actors, goals and the associated capabilities, as well as mitigation measures and response. Capability ID is a mere visualization; it doesn't yet impose the rules and doesn't model the secure constraints in Secure Tropos, correctly.

Based on the above, the SI* language is used to implement a rule (Secure Constraints). SI* is a flexible and powerful description language, and can define all elements within our privacy framework, for example:

Based on the secure Tropos implementation, the result is the privacy analysis using the test cases for each threat or actor’s interest. Test cases can also be validated, using the successful applicability of Secure Constraints. A test case can be defined, as follows,

Conclusion

The proposed framework is a set of privacy requirements, with definitions for all associated actors, goals, stakes, and inclusion of all entities, processes, and actions. The actor model defines the actors, their stakes, and capabilities. The framework is applied to the design of the privacy, enabling the system (hardware or software) using meta-model (performing the alignment). The Secure Tropos defines the secure constraints applicable and enforceable to the actors. The SI* is a description based and rule-based modeling language defining the Secure Tropos implementation. Finally, Test cases (the result of Secure Constraints) help validate the framework against privacy requirements in aware privacy system under design.

Validation

As a validation process, the primary aim from the proposed framework is to measure and prevent privacy leakage to validate the research findings. The main validation process is to compare the qualitative results from a systematically designed and validated privacy framework using Secure Tropos. Key strength of the application is that both, Privacy by design heuristics and Secure Tropos, are techniques based on engineering requirements for mitigating privacy leakage. In this research, a qualitative analysis methodology and adopted case study approach is used for the validation of findings.

The other validation process is to measure the amount of the prevented privacy leakage, in this research case study. This research work is based on the privacy-by-design principle that helps prevent privacy leakage, in this way, comparing the privacy-by-design engaged components with this research components, in the aim of the deceiver that this research meets its basic adopted principle. Resultant solution is validated using a publicly accessible network scenario in a lab environment, with the aid of physical equipments, as well as by using Simulation software.

I will use a dynamic technology that employs rule based secure Tropos language, taking scenario for modeling the privacy frameworks, as the basis, and drawing statistical and mathematical conclusions based on findings. Privacy framework will be validated in applying session management subsystem security and credential’s privacy mechanisms. The project will compare and contrast various security and credential’s privacy frameworks

to provide validity of optimal framework in a growing and increasingly emerging online set of platforms.

E-Voting system could fully be modeled and analyzed, using security Tropos for privacy analysis. In this business plan, the voter information and collected vote information privacy leakage is analyzed. Creating a simulation model in a simulation environment to run the tests is possible; however, the creation will definitely take much effort, since E-Voting system is a generic system.

Works Cited

Asnar, Y., Giorgini, P., Massacci, F., and Zannone, N. “ From trust to dependability through risk analysis.” In: Proc. of ARES’07 (2007): 19–26. Print.